Identity Theft

Assemblyman
Rick Keene

District Office
1550 Humboldt Road, Suite 4
Chico, CA 95928
Phone: (530) 895-4217
Fax: (530) 895-4219

Capitol Office
State Capitol
P.O. Box 942849
Sacramento, CA 94249-0003
Phone: (916) 319-2003
Fax: (916) 319-2103

Web
www.assembly.ca.gov/Keene

E-mail
Assemblymember.Keene
@assembly.ca.gov

California Legislature
Assembly
Rick Keene
ASSEMBLYMAN, 3RD DISTRICT

Dear Friend:

Many of us know people who have become victims of identity theft. We've heard their stories and have learned how devastating this crime can be, financially and emotionally.

This brochure describes the crime of identity theft. It contains important information on how to safeguard your privacy, and gives tips on protecting yourself from becoming a victim.

It also describes what steps to take if someone steals your identity.

Take the time to read this brochure and to follow some very simple steps to protect yourself and your family.

Sincerely,

Rick Keene
Assemblyman, 3rd District

credit card name account number exp. date

phone numbers: customer service fraud department

credit card name account number exp. date

phone numbers: customer service fraud department

credit card name account number exp. date

phone numbers: customer service fraud department

credit card name account number exp. date

phone numbers: customer service fraud department

credit card name account number exp. date

phone numbers: customer service fraud department

credit card name account number exp. date

phone numbers: customer service fraud department

credit card name account number exp. date

phone numbers: customer service fraud department

credit card name account number exp. date

phone numbers: customer service fraud department

bank name account number

phone number

bank name account number

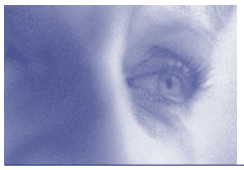
phone number

bank name account number

phone number

OTHER ACCOUNTS:

(examples: police fraud hotline, utilities, phone, calling cards, wireless, cable)



Identity Theft

Identity theft occurs when someone uses your personal information without your knowledge to commit fraud or theft. It can happen when the identity theft involves acquiring information like your name, bank account number or Social Security number to impersonate you.

Unlike your fingerprints, which are unique to you and cannot be given to someone else for their use, your personal data (especially your Social Security number, your bank account or credit card number, your telephone calling card number, and other valuable identifying data) can be used, if they fall into the wrong hands, to personally profit at your expense.

This guide will help you secure your information and allow you to spot identity theft sooner. If you already have been a victim of identity theft, please use the tips in this booklet to help you clear your name and protect yourself from further problems. Whether or not you are a victim, take the ID theft test on the back resource page to evaluate your vulnerability.

100 + points – More than 500,000 people will become victims of ID theft this year. You are at high risk. We recommend that you purchase a paper shredder, become more security aware in document handling, and start to question why people need your personal data.

50-100 points – Your odds of being victimized are about average, or slightly higher if you have good credit.

0-50 points – Congratulations! You have a high "IQ." Keep up the good work and don't let your guard down now.

Note: ID Theft test provided by Utility Consumers Action Network and Privacy Rights Clearinghouse.

test your "identity quotient"

Answer these questions, then total your points and use the chart on the next page to assess your risk of identity theft.

1) I receive several offers of pre-approved credit every week. **(5 points)** Add 5 more points if you do not shred them before putting them in the trash.
2) I carry my Social Security card in my wallet. **(10 points)**
3) I do not have a P.O. box or a locked, secured mailbox. **(5 points)**
4) I use an unlocked, open box at work or at my home to drop off my outgoing mail. **(10 points)**
5) I carry my military ID in my wallet at all times. **(10 points)**
6) I do not shred or tear banking and credit information before I throw it in the trash. **(10 points)**
7) I provide my Social Security number whenever asked, without asking questions as to how that information will be safeguarded. **(10 points)** Add **(5 points)** if you provide it orally without checking to see who might be listening.
8) I am required to use my Social Security number at work as an employee or student ID number. **(5 points)**
9) I have my Social Security number printed on my employee badge that I wear at work or in public. **(10 points)**
10) I have my Social Security number or driver's license number printed on my personal checks. **(20 points)**
11) I am listed in a "Who's Who" guide. **(5 points)**
12) I carry my insurance card in my wallet and either my Social Security number or that of my spouse is the ID number. **(20 points)**
13) I have not ordered a copy of my credit reports for at least 2 years. **(10 points)**
14) I do not believe that people would root around in my trash looking for credit or financial information. **(10 points)**

what is California doing about it?

The California Legislature and the Governor have taken action to prevent identity theft by passing laws that punish the criminals and help victims clear their names.

- Credit card companies must notify card holders of their right to prohibit disclosure of their personal information.
- Identity theft victims have the right to receive copies of any fraudulent credit, financial or other applications submitted using their identifying information.
- Credit reporting agencies are required to accept "security alerts" from consumers.
- Creditors can't sell a consumer debt to a debt collector if they have reason to believe the consumer is a victim of identity theft.
- The Office of Privacy Protection was created within the California Department of Consumer Affairs.
- Social Security numbers cannot be printed on material mailed to a person unless required by state or federal law.
- Consumers have the right to request and receive a record of all inquiries made to credit-reporting agencies for the past year.
- Consumers can have their names removed from credit card solicitation mailing lists for a minimum of two years.

How crooks get personal information

- They go through your trash can looking for unshredded papers. **Solution:** Always shred pre-approved credit applications, credit card receipts, bills and other financial information before throwing into the trash.
- They steal your mail. **Solution:** Quickly remove mail from your mailbox or use a post office box. Deposit outgoing mail at the post office or in another secure receptacle.
- They listen in on conversations you have in public. **Solution:** Always be aware of your surroundings.
- They buy the information, on the Internet or elsewhere, from someone who might have stole it. **Solution:** Regularly check your credit report for unauthorized accounts.
- They steal it from a loan or credit application you filled out or from files at a hospital, bank, school, car lot or business that you deal with. They may have obtained it from trash bins outside of such companies. **Solution:** Ask questions of businesses you deal with as to how your information will be used and disposed of once it is no longer needed. Be aware of the new state law that requires all banks and businesses to destroy paperwork containing customers' personal and financial information. The business must destroy it by shredding, erasing or modifying it in such a manner that it is unreadable or undecipherable. Customers can initiate civil action against the bank or business if they are victims of identity theft or fraud as a result of the business' failure to destroy paperwork properly.
- They get it from your computer, especially those without "firewalls." **Solution:** Always use firewall and virus protection on your computer if it is connected to the Internet. Keep all programs updated, including your operating system.
- The identity thief may be a friend or relative or someone who works with you who has access to your information. **Solution:** Do not allow anyone you don't fully trust to access to your computer or personal information.

- Contact the state office of the Department of Motor Vehicles to see if another license was issued in your name. If so, request a new license number and fill out the Department of Motor Vehicles' complaint form to begin the fraud investigation process.
- Obtain a description of the suspect (if known).
- Obtain witness information.
- What is your financial loss? Attach all supporting documents.
- Make note of this case number in your detailed history folder and reference it when you have contact with any business or law enforcement agency concerning this report. Depending on the location of the crime (where goods or services are obtained or delivered), an investigator may or may not be assigned to the case.
- If there are workable leads, such as witnesses and suspect information, an investigator may be assigned to the case. Unfortunately, cases probably will not be assigned to an investigator if there are no significant leads to identify the suspect.

Web resources

California Department of Consumer Affairs: www.dca.ca.gov

California ID Theft Database: www.caag.state.ca.us/idtheft/general.htm

CardCops: www.cardcops.com

Direct Marketing Association (Mail Fraud): www.e-mps.org

Direct Marketing Association (Phone Fraud): www.the-dma.org

Federal Trade Commission: www.ftc.gov

ID Theft Center: 858-693-7935, www.idtheftcenter.org

Privacy Rights Clearinghouse: 619-298-3396, www.privacyrights.org

Free Credit Report: www.AnnualCreditReport.com

Social Security Administration: www.ssa.gov

U.S. Postal Service: www.usps.gov

- Contact each of the three credit bureaus' fraud units to report identity theft. Ask to have a "Fraud Alert/Victim Impact" statement placed in your credit file asking that creditors call you before opening any new accounts.
- Request that a copy of your credit report be sent to you.
- If you have been charged with a crime committed by another person using your stolen identity, or if your identity has been mistakenly associated with a record of criminal conviction, you can register to enter your name into California's ID Theft Data Base. *(See web resources on page 8.)*

Credit bureaus

Trans Union: 800-888-4213, www.tuc.com
Fraud Division: 800-680-7289
Experian: 888-EXPERIAN, www.experian.com
Fraud Division: 888-397-3742
Equifax: 800-685-1111, www.equifax.com
Fraud Division: 800-525-6285, TDD 800-255-0056

- *Be aware that these measures may not stop new fraudulent accounts from being opened by the imposter. Request a free copy of your credit report every few months so you can monitor any new fraudulent activity. To request a credit report, go online to www.AnnualCredit Report.com.*

Credit bureaus

- Alert your banks to flag your accounts and contact you to confirm any unusual activity. Request a change of PIN and a new password.
- If you have any checks stolen or bank accounts set up fraudulently, report the crimes to the following companies:

CheckRite – 800-766-2748
Crosscheck – 707-586-0551
Equifax Check Systems – 800-437-5120
International Check Services – 800-526-5380
National Check Fraud Service – 843-571-2143
SCAN – 800-262-7771
Social Security Administration's Fraud Hotline – 800-269-0271
TeleCheck – 800-710-9898 or 800-927-0188

Secure your Social Security number

- Your Social Security number is the key to your credit and banking accounts, and is the prime target of criminals. Protect it! Release it only when absolutely necessary (for example, on tax forms, employment records, most banking, stock and property transactions). Do not carry your Social Security card in your purse or wallet.
- Do not have your Social Security number printed on your checks. Don't let merchants write it on your checks.
- Order your Social Security Earnings and Benefits Statement once a year to check for fraud.

Protect your personal information

- Do not carry your Social Security card or number, birth certificate, passport, passwords, or extra credit cards in your purse or wallet.
- Lock your home mailbox, use a mail slot instead of a mailbox, or use a post office box.
- When you pay bills, mail them at a post office. Do not leave them at your home mailbox, your workplace's out box, or even your neighborhood Postal Service mailbox. Neighborhood mail boxes can be burglarized.
- Instruct the post office not to process address change requests unless you personally deliver the request and show identification and proof of residence.
- Before you reveal any personal identifying information to a business, find out how it will be used and whether it will be shared. Ask if you can have your personal information kept confidential.
- Be careful sending personal information over Internet chat lines, e-mail or postings.

Credit cards

- Credit cards linked to any of your bank accounts (i.e., debit cards) are not afforded the same protections as a credit card (MasterCard, Visa, American Express), unless fraud is reported in a timely manner. To reduce your risk, reduce the number of credit cards you actively use to a bare minimum. Carry only one or two in your wallet.

- Cancel all unused accounts. Even though you do not use them, their account numbers are recorded in your credit report, which is full of data that can be used by identity thieves.
- Keep a list of all your credit cards, account numbers, expiration dates, and telephone numbers of the customer service and fraud departments. Keep this list in a secure place (not your wallet or purse) so you can quickly contact your creditors if your cards are stolen. Do the same with your bank accounts. Use the form on page 11 of this booklet to make the job easier.
- Never give out your credit card number or other personal information over the phone unless you have a trusted business relationship with the company and **you** initiated the call.
- Always take credit card receipts with you. Never toss them in a public trash container.

Protect your passwords and PINs

- When creating passwords and PINs (personal identification numbers), do not use the last four digits of your Social Security number, your birth date, middle name, pet's name, consecutive numbers, or anything else that could easily be discovered by thieves.
- Memorize all your passwords. Don't record them on anything in your wallet or purse.
- Shield your hand when using a bank ATM machine or making long-distance phone calls with your phone card. "Shoulder surfers" may be nearby.

Protect your financial documents

- Carefully review your credit card statements and phone bills, including cellular phone bills, for unauthorized use.
- Store your canceled checks in a safe place. In the wrong hands, they could reveal a lot of information about you, including the account number, your phone number and driver's license number. Never permit your credit card number to be written onto your checks. It's a violation of California law (California Civil Code 1725) and puts you at risk of fraud.

Be careful when you go online

- Use caution when disclosing checking account numbers, credit card numbers or other personal financial data at any web site or online service location unless you receive a secured authentication key from your provider.
- When you subscribe to an online service, you may be asked to give credit card information. When you enter any interactive service site, beware of con artists who may ask you to "confirm" your enrollment service by disclosing passwords or the credit card account number used to subscribe. Don't give out this information!

If you become a victim

- Keep a log of all your contacts and make copies of all documents.
- Contact all creditors, by phone and in writing, to inform them of the problem.

Sample Dispute Letter to a Credit Bureau

Date
Your name, Address, City, State ZIP Code
Institution Name, Address, City, State, ZIP Code
Ref: (account number if known)

To Whom It May Concern:
I am writing to dispute a fraudulent charge (or debit) attributed to my account in the amount of $_____. I am a victim of identity theft, and I did not make this charge (or debit). I am requesting the charge be removed (or the debit reinstated), that any finance or other charges related to the fraudulent amount be credited as well, and that I receive an accurate statement.

Enclosed are copies of (use this sentence to describe any enclosed information, such as a police report) supporting my position. Please investigate this matter and correct the fraudulent charge (or debit) as soon as possible, Thank you for your assistance.

Sincerely,